METHOD AND APPARATUS FOR COMPRESSING RABIN SIGNATURES

ABSTRACT

A method and apparatus are disclosed for compressing Rabin signatures. The disclosed compression scheme compresses a Rabin signature, s, for a user having a public key, n, based on a continued fraction expansion of s/n. The continued fraction expansion of s/n can be performed by (i) computing principal convergents, u_i/v_i, for i equal to 1 to k, of a continued fraction expansion of s/n, where k is a largest integer for which principal convergents are defined; establishing an index *l*, such that $v_l < \sqrt{n} \leq v_{l+1}$; and generating a compressed Rabin signature (v_l, m) for a message, m.